UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE GEICO CUSTOMER DATA BREACH LITIGATION	Case No. 1:21-cv-02210-KAM-SJB **CONSOLIDATED COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs Michael Viscardi, Kathleen Dorety, and William Morgan (collectively, "Plaintiffs") individually and on behalf the proposed Class, by and through Interim Co-Lead Class Counsel,[1] bring this Class Action Complaint against Defendants Government Employees Insurance Company d/b/a GEICO, GEICO Casualty Company, GEICO Indemnity Company, and GEICO General Insurance Company (collectively, "GEICO" or "Defendants"), and allege as follows:

INTRODUCTION

1. Every year, millions of Americans have their most valuable personal information disclosed and their privacy intruded upon because corporations seeking to maximize profits misuse their personal information, making the public vulnerable to fraudsters.

2. In an effort to stem the tide of such misuses and disclosures, and in recognition of the sensitivity of drivers' license information (and its utility to identity thieves), Congress passed the Drivers' Privacy Protection Act ("DPPA"), which restricts access to drivers' license

[1] This Court appointed the undersigned as Interim Co-Lead Class Counsel on April 8, 2022. ECF No. 59.

information, and mandates that private companies may only use it for limited, enumerated, purposes. Under the DPPA, private companies are legally required to protect from unauthorized access and exfiltration the personal information ("PI") that they obtain and use. In the DPPA, Congress specifically defines PI to include driver's license numbers. *See* 18 U.S.C. 2725(3).

3. Fraudsters harvest driver's license numbers because they are highly valuable pieces of PI. A driver's license can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[2] Driver's license numbers are particularly useful to identity thieves for applying for unemployment or other government benefits.

4. GEICO is best known for writing private passenger automobile insurance policies and is reportedly the nation's second-largest auto insurance company. GEICO offers coverages to insureds in all 50 states and the District of Columbia.[3] It markets its policies mainly by direct response methods whereby customers apply for coverage directly to the company via the internet or over the telephone. GEICO provides online insurance quotes to consumers through its online sales system on its publicly accessible insurance website.

5. Despite warnings about the severe impact of identity theft on Americans of all economic strata, companies—including GEICO—still put their own economic interests ahead of consumers' privacy interests.

---

[2] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach,* Forbes (Apr. 20, 2021, 11:57 A.M. EDT), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=146576a68658.

[3] The U.S. Securities and Exchange Commission, Form 10-K, (Dec. 31, 2019), https://www.berkshirehathaway.com/2019ar/201910-k.pdf.

6. Turning a blind eye to the limitations imposed by the DPPA, GEICO knowingly chose to obtain, use and disclose federally protected drivers' license information to grease the wheels of its online insurance sales. GEICO chose to add a feature to its existing online sales platform where an individual's driver's license number would *auto-populate* for anyone that would enter a bare minimum of publicly available information about that individual.

7. GEICO had offered online insurance quotes to applicants long before it incorporated this auto-population feature, but added the auto-population feature to its online sales system in order to gain competitive advantage in its sales process. GEICO's conduct is motivated by its desire to entice customers to complete applications for insurance.

8. By adding the auto-population feature to its online quoting process, which GEICO knowingly chose to do, GEICO intended to make the displayed information, which it obtained and used to create the feature, easily accessible to anyone who entered basic information into its system. GEICO did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. GEICO did not impose effective security protocols to prevent automated bots from accessing consumers' PI. Thus, GEICO effectively posted consumers' driver's license numbers, including Plaintiffs' and the Class Members', on the internet's "windshield," for all digital passers-by with a few bits of others' PI to see.

9. GEICO's decision quickly caught the attention of identity thieves, who mined GEICO's website and obtained private drivers' license information about hundreds of thousands of consumers, including Plaintiffs.

10. In a document entitled "Notice of Data Breach" dated April 9, 2021 (the "Notice"), GEICO informed affected victims "of an incident that affected the confidentiality" of their PI, and that the so-called incident had occurred between November 24, 2020 and March 1, 2021 (the "Data

Disclosure"). According to the Notice, unauthorized third parties accessed driver's license numbers through GEICO's online sales system: "fraudsters used information about you – which they acquired elsewhere – to obtain unauthorized access to your driver's license number through the online sales system on our website." GEICO acknowledged that information "could be used to fraudulently apply for unemployment benefits" under the victims' names. The Notice further instructed those affected to review any mailings they receive from their state's unemployment agency/department and to contact the agency/department if there is any chance fraud is being committed. The Notice did not state that the "information acquired elsewhere" was simply a person's name, address and date of birth which is publicly available through a simple Google search or accumulated in data bases and widely available on the Internet. Through the Notice, GEICO also acknowledged that it had obtained and used the information in the design and creation of the new online sales feature.

11. GEICO sent Notices to Plaintiffs Viscardi, Dorety, and Morgan, thus, their sensitive driver's license numbers were exposed to criminals. All three named Plaintiffs have also received notifications from the New York Department of Labor that fraudulent unemployment claims have been filed in their names following GEICO's Data Disclosure. The Plaintiffs have also experienced other instances of identity theft logically and temporally related to Defendants' exposure of their driver's license numbers.

12. While the Notice indicated that GEICO secured the affected website "as soon as it became aware of the issue" and that it has implemented additional security enhancements to help prevent future fraud and illegal activities on its website, unfortunately for Plaintiffs, the damage to their privacy had already been done. As a result of GEICO's Data Disclosure, Plaintiffs' privacy has been invaded, their sensitive drivers' license information is now in the hands of criminals, and

they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from identity theft and fraud.

13. In order to redress GEICO's illegal profit-seeking conduct, Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members") who had their driver's license information used and exposed as a result of GEICO's sales efforts and during GEICO's Data Disclosure. Plaintiffs, on behalf of themselves and the Class Members, seek remedies, including monetary damages and injunctive relief (including relief under the federal Declaratory Judgment Act), for GEICO's violation of the DPPA, negligence, negligence per se, invasion of privacy (intrusion upon seclusion), and violations of New York's consumer protection law ("GBL").

PARTIES

Plaintiff Michael Viscardi

14. Plaintiff Michael Viscardi is a citizen of the state of New York and resides in Holtsville, New York.

15. On or about April 9, 2021, GEICO sent, and Plaintiff Viscardi subsequently received, the Notice, confirming that he was impacted by GEICO's Data Disclosure, and that his driver's license number was obtained, used and disclosed by GEICO.

16. The Notice stated that "between November 24, 2020 and March 1, 2021, fraudsters used information about [Plaintiff] – which they acquired elsewhere – to obtain unauthorized access to [Plaintiff's] driver's license number through the online sales system on [GEICO's] website." Thus, the Notice acknowledges that the fraudsters also had other information about Plaintiff

Viscardi that they had "acquired elsewhere," and that they used to access and link Plaintiff Viscardi's driver's license number to that other information.

17. The Notice further stated: "We have reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name."

18. On or about February 12, 2021, (after GEICO's Data Disclosure, but before GEICO sent him the Notice), Plaintiff Viscardi received a letter from the New York Department of Labor notifying him of a fraudulent claim for unemployment benefits made in his name.

19. On or about February 14, 2021, (also after GEICO's Data Disclosure, but before GEICO sent him the Notice), Plaintiff Viscardi received another letter from the New York Department of Labor informing him that he was eligible for Pandemic Unemployment Assistance.

20. Plaintiff Viscardi is self-employed and did not apply for unemployment benefits. Plaintiff Viscardi's PI, i.e., his driver's license number, was disclosed in GEICO's Data Disclosure and was used to make fraudulent claims for unemployment benefits in his name, as GEICO admitted might occur.

21. Plaintiff Viscardi subsequently received a letter from his bank, informing him of an attempt to transfer funds from his joint bank account to an unauthorized account.

22. This fraud and attempted identity theft occurred after GEICO's Data Disclosure, but nearly two months before Defendants sent Plaintiff the Notice. This fraud and identity theft is temporally and logically connected to the data derived from GEICO's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." GEICO disclosed Plaintiff Viscardi's driver's license number shortly before he experienced two different attempts at fraud and identity theft: a claim for pandemic-related unemployment benefits and an attempt to

transfer funds from his bank account to an unauthorized account. All are forms of identity theft specifically linked to fraudulently used driver's license numbers.

23. In the summer of 2021, Plaintiff Viscardi received a text message alert from Chase Bank regarding a charge on his credit card of about a couple hundred dollars, asking him to confirm if the charge was made by him. The charge on the credit card was not made by Plaintiff Viscardi or his wife and he notified the bank that it was fraudulent. The bank opened an investigation regarding the charge, closed Plaintiff Viscardi's credit card and issued him a new card.

24. On or about December 3, 2021, Plaintiff Viscardi received an e-mail identifying that there was unusual activity on his Bank of America VISA credit card. He wound up suffering three fraudulent charges of approximately $1,000 total. His credit card was closed and he was reimbursed for these losses, but Plaintiff was without the use of his payment card for a number of days.

25. Plaintiff Viscardi has taken (and continues to take) considerable precautions to protect the unauthorized dissemination of his PI. To date, he has spent approximately 90 hours monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, as a result of GEICO's disclosure of his PI, Plaintiff Viscardi's sensitive information was disseminated without his consent, has already been fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

26. As a result of GEICO's Data Disclosure, Plaintiff Viscardi suffered injury and/or damages, including but not limited to actual identity theft; time and expenses interacting with government agencies, and general mitigation efforts spent on monitoring credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of

his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, as a result of GEICO's Data Disclosure, Plaintiff Viscardi now faces a substantial risk that unauthorized third parties will further misuse his PI.

Plaintiff Kathleen Dorety

27. Plaintiff Dorety is a citizen of the state of New York and resides in Springwater, New York.

28. On or about April 9, 2021, GEICO sent, and Plaintiff Dorety subsequently received, the Notice, confirming that she was impacted by GEICO's Data Disclosure, and that her driver's license number was obtained, used and disclosed by GEICO.

29. The Notice Plaintiff Dorety received contained the same language described above: that "between November 24, 2020 and March 1, 2021, fraudsters used information about [Plaintiff] – which they acquired elsewhere – to obtain unauthorized access to [Plaintiff's] driver's license number through the online sales system on [GEICO's] website." Thus, the Notice acknowledges that the fraudsters also had other information about Plaintiff Dorety that they had "acquired elsewhere," and that they used to access and link Plaintiff Dorety's driver's license number to that other information.

30. The Notice further stated: "We have reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name."

31. On or about March 23, 2021, (after GEICO's Data Disclosure, but before GEICO sent her the Notice), Plaintiff Dorety received a letter from the New York Department of Labor notifying her of a fraudulent claim for unemployment benefits made in her name.

32. Plaintiff Dorety contacted the Livingston County Sheriff's office and filed a police report the same day.

33. Plaintiff Dorety is employed and did not apply for unemployment benefits. Plaintiff Dorety's PI, i.e., her driver's license number, was disclosed in GEICO's Data Disclosure and was used to make a fraudulent claim for unemployment benefits in her name, as GEICO admitted might occur.

34. In May 2021, Plaintiff Dorety's husband received a checkbook in the mail from TD Bank, referencing a checking account that he did not open. Plaintiff Dorety subsequently learned that a TD Bank account had been fraudulently opened in her name as well. She filed another police report and spent substantial time interacting with TD Bank to ensure that she and her husband were not responsible for transactions make on the fraudulently opened accounts.

35. This fraud and identity theft is temporally and logically connected to the data derived from GEICO's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." GEICO disclosed Plaintiff Dorety's driver's license number shortly before she experienced two different attempts at fraud and identity theft: a claim for unemployment benefits and an attempt to open an unauthorized account. Both are forms of identity theft specifically linked to fraudulently used driver's license numbers.

36. Plaintiff Dorety has taken (and continues to take) considerable precautions to protect the knowing disclosure of her PI. To date, she has spent numerous hours monitoring accounts, making police reports, calling financial institutions, and otherwise dealing with the fallout of GEICO's Data Disclosure. Unfortunately, as a result of GEICO's Data Disclosure, Plaintiff Dorety's sensitive information was disseminated without her consent, has already been fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

37. As a result of GEICO's Data Disclosure, Plaintiff Dorety suffered injury and/or

damages, including but not limited to actual identity theft; time and expenses interacting with government agencies, and general mitigation efforts spent on monitoring credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PI; and injury to her privacy. Additionally, as a result of GEICO's Data Disclosure, Plaintiff Dorety now faces a substantial risk that unauthorized third parties will further misuse her PI.

Plaintiff William Morgan

38. Plaintiff Morgan is a citizen of the state of California, but in 2021, he resided in Brooklyn, New York.

39. On or about April 9, 2021, GEICO sent, and Plaintiff Morgan subsequently received, the Notice, confirming that he was impacted by GEICO's Data Disclosure, and that his driver's license number was obtained, used and disclosed by GEICO.

40. The Notice Plaintiff Morgan received contained the same language described above: that "between November 24, 2020 and March 1, 2021, fraudsters used information about [Plaintiff] – which they acquired elsewhere – to obtain unauthorized access to [Plaintiff's] driver's license number through the online sales system on [GEICO's] website." Thus, the Notice acknowledges that the fraudsters also had other information about Plaintiff Morgan that they had "acquired elsewhere," and that they used to access and link Plaintiff Morgan's driver's license number to that other information.

41. The Notice further stated: "We have reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name."

42. In March 2021 (after GEICO's Data Disclosure, but before GEICO sent him the

Notice), Plaintiff Morgan received a letter from the New York Department of Labor notifying him of a fraudulent claim for unemployment benefits made in his name.

43. Plaintiff Morgan is retired and did not apply for unemployment benefits. Plaintiff Morgan's PI, i.e., his driver's license number, was disclosed in GEICO's Data Disclosure and was used to make a fraudulent claim for unemployment benefits in his name, as GEICO admitted might occur.

44. After receiving the notice of the fraudulent unemployment application and the notice from Defendant, Plaintiff Morgan underwent the time and effort to freeze his credit in an effort to thwart future fraud.

45. This fraud and identity theft is temporally and logically connected to the data disclosed in GEICO's Data Disclosure in the same way that other data breach cases have found to be "fairly traceable." GEICO disclosed Plaintiff Morgan's driver's license shortly before he experienced an attempt at fraud and identity theft: a claim for unemployment benefits. This form of identity theft is specifically linked to fraudulently used driver's license numbers.

46. Plaintiff Morgan has taken (and continues to take) considerable precautions to protect the knowing disclosure of his PI. To date, he has spent numerous hours monitoring accounts, freezing his credit, and otherwise dealing with the fallout of GEICO's Data Disclosure. Unfortunately, as a result of GEICO's Data Disclosure, Plaintiff Morgan's sensitive information was disseminated without his consent, has already been fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

47. As a result of GEICO's Data Disclosure, Plaintiff Morgan suffered injury and/or damages, including but not limited to actual identity theft; time and expenses interacting with government agencies, and general mitigation efforts spent on monitoring credit and for identity

theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, as a result of GEICO's Data Disclosure, Plaintiff Morgan now faces a substantial risk that unauthorized third parties will further misuse his PI.

GEICO Defendants

48. Defendants Government Employees Insurance Company, GEICO Casualty Company, GEICO Indemnity Company, and GEICO General Insurance Company are Maryland corporations with their principal places of business in Chevy Chase, Maryland. GEICO is authorized to conduct business in the State of New York. GEICO is one of the largest auto insurance companies in the United States, boasting assets of more than $32 billion.[4]

JURISDICTION AND VENUE

49. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because at least one Plaintiff and Defendants are citizens of different states. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims. Subject matter jurisdiction is also based upon the Federal Trade Commission Act ("FTCA"). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

50. The Court has personal jurisdiction over Defendants because Defendants conduct significant business in the state of New York, thus availing themselves of New York's markets by

[4] *Id.*

selling auto insurance policies; have sufficient minimum contacts with the state of New York; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in New York.

51. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, were directed to, and/or emanated from this district; Defendants transact substantial business and have agents in this district; a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this judicial district; and because Plaintiffs reside within this district.

FACTUAL ALLEGATIONS

A. GEICO Collects Vast Amounts of Sensitive PI from Consumers and Third Parties

52. GEICO primarily offers private passenger automobile insurance to individuals in all 50 states and the District of Columbia. GEICO also insures motorcycles, all-terrain vehicles, recreational vehicles, boats and small commercial fleets and acts as an agent for other insurers who offer homeowners, renters, life and identity management insurance to individuals who desire insurance coverages other than those offered by GEICO.[5]

53. GEICO collects and stores vast amounts of personal information and sensitive data from prospective clients, current and former customers, and other consumers, as part of its regular business practices. Included in this information is highly sensitive driver's license numbers. For example, "during the quoting, application, or claims handling processes," GEICO obtains an individual's "Name, Address, Phone number, Social Security number, *Driver's license number*, Date of birth,"[6] among other sensitive personal information. (Emphasis added.) Discovery will show that during the insurance claims process, GEICO also requires submission of similar personal

[5] *Id.*

[6] GEICO, *Privacy Policy, Geico Respects Your Privacy*, https://media.geico.com/legal/privacy_policy.htm.

information in connection with insurance processing claims, including from individuals who are not GEICO policyholders but who are involved in a claim being handled by GEICO, such as drivers involved in accidents with GEICO insureds.

54. GEICO's marketing is primarily through direct response methods in which consumers submit applications for insurance directly to Defendants via the Internet or by telephone, and to a lesser extent, through captive agents.

55. Competition for private passenger automobile insurance, which is substantial, tends to focus on price and level of customer service provided.

56. Like other insurance providers, GEICO has an online sales system available to all persons capable of accessing it via the internet. Visitors to GEICO's insurance website can get a quote instantly after providing some PI.

57. Defendants' quoting feature uses the information entered by the website visitor, combines it with additional information Defendants have or that Defendants can access from third-party prefill services, and then automatically displays the additional information to the visitor as part of the quote process.

58. Specifically, Defendants' quoting feature asks any visitor to the site for their name, date of birth, and address. Once a visitor enters that information, Defendants' system auto-populates the quotation with driver's license information from Defendants' own databases or from third-party prefill services and makes that information visible to the person entering the information on the GEICO quote website.

59. A person's name, date of birth, and address are data that are publicly available and easily attained. It is common knowledge and GEICO knew that this information is compiled in

multitudes of different databases available on the Internet, often at no cost.[7]

60. An automated process, or "bot," was used on the instant quote feature to obtain Plaintiffs' and Class Members' driver's license numbers, which includes many people who never applied for insurance with Defendants or were even necessarily aware of Defendants' existence. In other words, unauthorized parties availed themselves of the PI Defendants made publicly available via their instant quote feature on a wholesale basis.

61. Defendants' online sales system did not require verification that the person or automated process accessing the system was actually the individual for whom the information was being entered. In addition, Defendants' online sales system did not employ effective, industry-standard security measures to detect whether the website visitor was, in fact, a "bot" or automated process rather than an individual person. Instead, Defendants configured their online sales system to provide PI—including driver's license numbers—when anyone, including bots, just entered commonly known information such as a person's name, date of birth, and address. Thus, Defendants' online sales system was purposefully and knowingly set up to allow any site visitor, including bots, to access and view PI including driver's license numbers of anyone about whom Defendants had collected or could access that PI simply so that GEICO could more easily sell its main product.

B. Defendants Contravened the Purpose of the Driver's Privacy Protection Act

62. Prior to the enactment of the Driver's Privacy Protection Act, Congress found that

[7] For example, "[s]ince approximately 2009, MyLife has purchased public record data about individuals from data brokers. … MyLife uses that data to create a 'public listing' or profile for these individuals, which can be accessed through its website, www.mylife.com. … On its website, MyLife has profiles purporting to cover at least 320 million individuals. ... Information that may be available through a *free search may include: name; city and state of residence; ... email address, and mailing address associated with the profile; date of birth*; …." *United States v. MyLife.com, Inc.*, No. CV 20-6692-JFW(PDX), 2021 WL 4891776, at *2 (C.D. Cal. Oct. 19, 2021) (citations omitted) (emphasis added).

most states freely turned over DMV information to whomever requested it with only few restrictions. 137 Cong. Rec. 27,327 (1993).

63. Due to this lack of restrictions, Congress grew concerned that potential criminals could easily obtain the private information of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

64. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an upcoming actor, after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

65. In light of public outrage over the Schaeffer murder and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

66. Additionally, in enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being

released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, No. 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The release of private information like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

67. As such, Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record." *Chamber of Com. of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1).

68. By knowingly using the PI of Plaintiffs and the Class for sales and marketing purposes, and by knowingly disclosing that PI to the public, Defendants ran afoul the purpose of DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendants' actions constituted a concrete injury and particularized harm to Plaintiffs and members of the Class, that would not have happened but for Defendants' failure to adhere to the DPPA. Plaintiffs were harmed by the public disclosure of their private facts in addition to the other harms enumerated herein.

C. The Data Use and Disclosure and Its Impact

69. In the Notice dated April 2021, GEICO notified consumers that their sensitive PI—namely, driver's license numbers—was compromised in a security incident, which it described as follows:

> We recently determined that between November 24, 2020 and March 1, 2021, fraudsters used information about you – which they acquired elsewhere – to obtain unauthorized access to your driver's license number through the online sales system

> on our website. We have reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name.[8]

70. While the Notice indicates that "as soon as it became aware of the issue" GEICO "secured the affected website and worked to identify the root cause of the incident," the Notice does not provide the date when GEICO learned of or "became aware of" the incident. Instead, the Notice merely states that GEICO "recently determined" that the incident had occurred and provides no further details.

71. GEICO's use of the driver's license numbers, its Data Disclosure through its online sales platform, and its violation of the law, assisted an ongoing and concerted campaign by fraudsters to engage with insurers' online quoting platforms to obtain driver's license numbers. On February 16, 2021 the New York State Department of Financial Services ("DFS") issued an alert regarding an ongoing systemic and aggressive campaign to engage with public-facing insurance websites—particularly those that offer instant online automobile insurance quotes—to obtain non-public information, in particular unredacted driver's license numbers.[9] According to the alert, the unauthorized collection of driver's license numbers appears to be part of a growing fraud campaign targeting pandemic and unemployment benefits. DFS first became aware of the campaign when it received reports from two auto insurers in December 2020 and January 2021 that cybercriminals were targeting their websites that offer instant online automobile insurance quotes to obtain unredacted driver's license numbers.

72. Insurers' instant online auto quoting websites are the primary entry point for cybercriminals to access consumers' PI. As the industry has accelerated adoption of faster-quoting

---

[8] Geico, *Notice of Data Breach* (Apr. 9, 2021), State of California Department of Justice, https://oag.ca.gov/system/files/DL3_IndNoticeLttr_CA_Redacted.pdf.

[9] Department of Financial Services, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn.

processes and tools to achieve competitive advantage, new vulnerabilities have opened.[10] According to DFS, insurers noticed an unusually high number of abandoned quotes or quotes not pursued after the display of the estimated insurance premium. On the instant quote websites, "criminals entered valid name, any date of birth and any address information into the required fields" and "then displayed an estimated insurance premium quote along with partial or redacted consumer [PI] including a driver's license number. The attackers captured the full, unredacted driver's license numbers without going any further in the process and abandoned the quote."[11] Of-course, GEICO need not use driver's license numbers on a sales platform, or disclose this information to the public, to underwrite any auto insurance policy.

73. In January 2021, DFS alerted approximately a dozen entities maintaining such websites that they were likely targets of hackers looking to gain access to New Yorkers' PI, specifically driver's license numbers. Following the alert, six more insurers apparently reported to DFS the malicious targeting of their websites—two of which insurers reported that the fraudsters failed to gain access to PI and four of which reported that the fraudsters did gain access to PI or that their investigation was still ongoing. In the alert, DFS did not name the websites affected or the insurers.

74. The increase in interest in driver's license numbers is, in part, a product of the changes brought on by the COVID-19 pandemic, as various types of financial transactions that used to be conducted exclusively in person have been transferred online. Some states are also allowing residents to use expired driver's licenses for various purposes for an extended period, due

[10] *Id.*
[11] *Id.*

to difficulty in securing the in-person DMV appointments necessary to renew them.[12]

75. Unsurprisingly, fraudulent unemployment claims have spiked during the pandemic, as more money has become available to displaced workers and the requirements for filing have eased. Many states have paid out tens of millions of dollars to scammers, a phenomenon largely driven by the unauthorized use of fraudulently obtained PI. Hackers have been caught using not just sensitive personal data for these fraudulent unemployment claims, but also hacking into existing unemployment accounts to change bank payment information.[13]

76. The United States Department of Labor estimates that pre-pandemic fraudulent unemployment claims accounted for about 10% of all filings.[14] A normal yearly cost for fraudulent unemployment claims is about $3 billion; recent reports indicate that this number ballooned to $200 billion during the pandemic. Fraudulent first-time claims drove a lot of this activity, but experts expect the problem to persist even as most Americans head back to work. Some will fail to notify the state unemployment office of their change in employment status, creating an opening for scammers.

77. GEICO knew that it was using driver's license information on its online sales platform. GEICO also knew that this platform was created and maintained in a way that allowed fraudsters to plug in readily and publicly available, basic and publicly available personal information of other persons, and that the website would auto-populate driver's license information

---

[12] CPO Magazine, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited May 20, 2022).

[13] *Id.*

[14] Megan DeMatteo, *Unemployment fraud costs victims $200 billion annually in the U.S. – here's how to protect yourself*, CNBC (Apr. 27, 2021), https://www.cnbc.com/select/how-to-protect-yourself-from-unemployment-fraud/.

into its quoting tool once that basic information is entered. Indeed, GEICO was responsible for its website, including its design and design features. GEICO thus knew, inferably knew, or should have known, that its website and the website's auto-populate feature disclosed consumers' driver's license number to anyone.

78. Not only did GEICO know that it was using driver's license numbers to sell insurance, and that it was disclosing driver's license numbers to the public, but it also failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumers' PI, and failed to implement basic safeguards to protect the security, confidentiality, and integrity of that information. By adding the auto-population feature to its online quoting process, which GEICO knowingly chose to do, GEICO intended to use the driver's license numbers and make the displayed information easily accessible to anyone who entered basic information into its system. GEICO did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. GEICO did not impose effective security protocols to prevent automated bots from accessing consumers' PI. Thus, GEICO knowingly used and posted consumers' driver's license numbers directly to all members of the public.

D. Defendants Acknowledged That the Use of Data and Its Data Disclosure Creates a Substantial Risk of Identity Theft and Fraud

79. The extent, scope, and impact of GEICO's use of the data and its Data Disclosure on its customers and other consumers remains uncertain. Nevertheless, the harm caused to Plaintiffs and Class Members by GEICO's Use of the information and its Data Disclosure is already apparent. Criminals now possess Plaintiffs' and Class Members' driver's license numbers, and their only purpose in obtaining and possessing that information is to monetize that data by selling it on the darknet or dark web, or using it to commit other types of fraud.

80. Defendants' Notice specifically admonished Plaintiffs and Class Members to take

mitigation steps: "If you receive any mailings from your state's unemployment agency/department, please review them carefully and contact that agency/department if there is any chance fraud is being committed." The Notice also states: "[W]e encourage you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity." The Notice includes an attachment recommending vigilance for incidents of fraud or identity theft, explaining how to report such incidents to the Federal Trade Commission and/or to one's state attorney general, and explaining how to obtain one's credit reports.

81. After receiving the Notice about GEICO's Data Disclosure, it is reasonable for Plaintiffs and Class Members to believe that the risk of future harm (including identity theft or fraud) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. Defendants' specific instructions and warnings in the Notice relate to the fact that hackers take driver's license numbers for the purpose of committing fraud in the name of the person whose license number is taken. This has already occurred, and there have been numerous reports of state unemployment benefits fraud linked to GEICO's Data Disclosure.

E. The PI GEICO Obtained, Used and Then Disclosed in Its Data Disclosure Is Highly Valuable to Fraudsters

82. It is well known amongst companies that store or have access to sensitive PI that driver's license numbers are valuable and frequently targeted by criminals. The PI that Defendants voluntarily disclosed via their online sales system in violation of state and federal law is very valuable to phishers, identity thieves, cyber criminals, and other fraudsters, especially at this time where unprecedented numbers of criminals are filing fraudulent unemployment benefit claims, and driver's license information is uniquely connected to the ability to file such claims and commit other financial fraud. Unsecured sites that contain or transmit PI such as driver's license numbers

require notice to consumers when the data is stolen because it can be used to commit identity theft and other types of fraud.

83. The driver's license numbers disclosed in GEICO's Data Disclosure are significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. By contrast, the information disclosed in GEICO's Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards or take out loans, especially student loans. The driver's license numbers disclosed in GEICO's Data Disclosure are also more valuable because they are long lasting, and difficult to change.

84. With access to an individual's driver's license number, criminals can commit all manner of fraud, including: obtaining government benefits in the victim's name, filing fraudulent tax returns using the victim's information, or obtaining a driver's license or official identification card in the victim's name but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name, and may even give the victim's driver's license number during an arrest, resulting in an arrest warrant being issued in the victim's name.[15] They can also use the driver's license when receiving a ticket or to provide to an accident victim, to replace or access account information on social media sites, to obtain a mobile phone, to dispute or approve a SIM swap, to redirect U.S. mail, to gain unauthorized access to the United States, to claim a lost or stolen passport, to use as a baseline to obtain a Commercial Driver's License, or to engage in phishing or other social engineering scams.

85. Fraudsters often aggregate information taken from data security incidents to build

[15] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited on May 20, 2022).

profiles on individuals. These profiles combine publicly available information with information discovered in previous data security incidents and exploited vulnerabilities. There are few data security incidents that provide a comprehensive snapshot of any one individual person. Unique and persistent identifiers such as Social Security numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to forging an identity. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "fullz"[16] profile can be obtained.

86. There is no legitimate or legal reason for anyone to use Defendants' website to acquire driver's license information on Plaintiffs and the Class Members. Dark Net Markets ("DNM(s)"), or the "dark web," is a heavily encrypted part of the internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity. When malicious actors obtain ill-gotten PI, that information often ends up on the dark web because the malicious actors buy and sell that information for profit.[17] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

87. Any non-public data, especially government issued identification numbers like a

[16] "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information for an entity or individual.

[17] *Shining a Light on the Dark Web with Identity Monitoring*, Identity Force (Dec. 28, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May 20, 2022).

driver's license or non-driver's identification number, has criminal value.[18] For example, a fake U.S. citizenship kit for sale: passport, SSN, driver's license, and birth certificate, is offered on the dark web for 0.218 bitcoin (or $1,400 at the time) and a stolen/fake driver's license (by U.S. state) for $200.[19]

88. Prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices when they reach the "flea market sites." DNMs are a downstream "flea market" for data to be sold, usually not by the original threat actor or criminal group. It is a dumping ground, usually after the data has been exploited. The value of stolen driver's license information currently has a DNM value of $1 per license. This was re-verified on March 3, 2022, accessing several DNM using a trusted identity. Social Security numbers, once considered the "gold standard" of identity fraud, are also selling for $1 per number in those same markets. This illustrates the value of driver's license information to cybercriminals and people committing identity fraud. According to popular DNMs, cyber criminals value driver's license numbers equally to Social Security numbers.

89. In some ways, driver's license numbers are even more attractive than Social Security numbers to threat actors and more dangerous to the consumer when disclosed. Unlike a Social Security number, a driver's license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive

---

[18] Identity Theft Resource Center, *Can Someone Steal Your Identity From Your Driver's License?* (Feb. 19, 2021) https://www.idtheftcenter.org/can-someone-steal-your-identity-from-your-drivers-license/ (last visited May 20, 2022).

[19] Daniel Shkedi, *Heart of Darkness: Inside the Darknet Markets that Fuel Financial Cybercrime*, BioCatch, https://web.archive.org/web/20210905231044/https://www.biocatch.com/blog/financial-cybercrime-darknet-markets (last visited May 20, 2022).

identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend immediate notice and replacement, and that identity theft protections are put in place for a minimum of 3 years. Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

90. Blogger Gayle Sato from the national credit reporting company Experian emphasized the value of driver's license information to thieves and cautioned:

> Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.[20]

91. In fact, according to the data privacy and cyber security publication CPO Magazine:

> To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: ". . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.[21]

---

[20] Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?* Experian (Nov. 3, 2021) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[21] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine (April 23, 2021) https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

92. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application: "Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name."[22]

93. The use of stolen driver's license numbers to obtain unemployment benefits under another person's name was confirmed by the New York State DFS on February 16, 2021 industry letter described above, which stated that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [PI, including] websites that provide an instant quote. . . . [and that] DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits."[23] New York State DFS has notified all three Plaintiffs named here that fraudulent unemployment claims have been filed in their names.

94. The process that was used to extract the data from Defendants' website was likely automated. The identity thieves have demonstrated the value they place on the driver's license

---

[22] Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TechCrunch (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name.

[23] New York State Department of Financial Services, *Industry Letter* (Feb. 16, 2021) https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (last accessed March 7, 2022).

numbers by engaging in a systematic and businesslike process for collecting them from GEICO's Data Disclosure and from additional insurers' websites offering instant quotes.

95. The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that, when criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name, this type of identity fraud can be the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime.[24] The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[25]

F. Defendants Failed to Comply with Federal Trade Commission Requirements

96. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and knowing disclosures of information via public websites, and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

97. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

---

[24] *See* United States Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), http://www.gao.gov/assets/270/262899.pdf.

[25] *Id.*

[26] Federal Trade Commission, *Start With Security: A Guide for Business*, (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

practices for business.[27] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[28]

98. Also, the FTC recommends companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[29]

99. Highlighting the importance of protecting against these types of disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[30]

---

[27] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[28] *Id.*

[29] *Start With Security*, *see supra* n.35.

[30] *See* Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

100. Through negligence in designing and implementing their online quoting platform and securing Plaintiffs' and Class Members' PI, Defendants knowingly allowed the general public—and thieves—to utilize their online sales system to obtain access to and collect individuals' PI. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiffs' and Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

G. Plaintiffs' Injuries—Attempts to Secure PI After GEICO's Data Disclosure

101. Defendants admitted in the Notice that there was disclosure of Plaintiffs' and Class Members' driver's license numbers to third parties. Defendants also concede that this disclosure created imminent harm to Plaintiffs and Class Members, specifically stating it "believe[s] that this information could be used to fraudulently apply for unemployment benefits in your name." GEICO tasked Plaintiffs and Class Members with reviewing written communications from state unemployment agencies for fraudulently filed applications, and offered a year of credit monitoring. These measures are woefully inadequate and do not absolve GEICO of its violations of the DPPA and other laws alleged herein.

102. Plaintiffs and Class Members have been, and will continue to be, injured because GEICO disclosed their personal information, and they are now forced to spend time monitoring their credit and governmental communications—per Defendants' instructions—guarding against identity theft, and resolving fraudulent claims and charges because of Defendants' actions and/or inactions.

H. Plaintiffs and Class Members Suffered Additional Damages

103. Plaintiffs and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

104. The ramifications of Defendants' disclosure and failure to keep individuals' PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.[31]

105. Plaintiffs' and Class Members' driver's license numbers are private, valuable, and sensitive in nature as they can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendants did not obtain Plaintiffs' and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

106. Defendants' decision to expose Plaintiffs and Class Members to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's driver's license number by utilizing Defendants' front-facing online instant quote platform left Plaintiffs and Class Members with no ability to protect their sensitive and private information.

107. Defendants had the resources necessary to prevent their Data Disclosure, but did not implement data security measures, despite their obligations to protect Plaintiffs' and Class Members' PI from unauthorized disclosure.

108. Despite the known risk of data security incidents and data leaks, and the widespread publicity and industry alerts regarding other similar data security events, Defendants failed to take reasonable steps to adequately secure GEICO's website and publish it in a manner that did not hand over Class Members' driver's license numbers to unauthorized third-parties, leaving GEICO

[31] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

customers and other consumers, including Plaintiffs and Class Members, exposed to risk of fraud and identity theft.

109. Defendants were, and at all relevant times have been, aware that the PI GEICO handles and stores in connection with its services is highly sensitive. Because GEICO is a company that provides insurance services involving highly sensitive and identifying information, Defendants were aware of the importance of safeguarding that information and protecting its websites, systems, and products from security vulnerabilities.

110. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and they were alerted to the risk associated with knowingly providing driver's license numbers to members of the public on GEICO's website.

111. Defendants knowingly obtained, used, disclosed and compromised Plaintiffs' and Class Members' PI by creating the online sales platform with the auto-populate feature, voluntarily transmitting it directly to any member of the public, including fraudulent actors. GEICO failed to take reasonable steps against an obvious threat. GEICO designed and implemented its own website using driver's license information, which included the instant quote feature that auto-populated Class Members' drivers' license numbers in response to the input of very basic publicly available consumer information was a feature that GEICO knowingly included on its website.

112. Had Defendants never used the information to sell auto insurance or never included this feature on its sales platform, it would have prevented the disclosure, unauthorized access, and ultimately, the fraudulent use and possible fraudulent use of the PI.

113. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would

have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of GEICO's Data Disclosure on their lives.

114. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[32]

115. As a result of Defendants' Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at imminent risk of suffering:

a. The compromise, publication, fraudulent, and/or unauthorized use of their PI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of GEICO's Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PI, which remains in the possession of Defendants and is subject to further compromise so long as Defendants fail to undertake appropriate measures to protect the PI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of GEICO's Data

[32] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, (December 2013) https://www.bjs.gov/content/pub/pdf/vit12.pdf.

Disclosure for the remainder of the lives of Plaintiffs and Class Members.

116. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further disclosure, misappropriation, and theft.

117. To date, other than providing 12 months of credit monitoring and identity protection services, Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do the following:

- "be vigilant for incidents of fraud or identity theft"
- "by reviewing your account statements and credit reports for any unauthorized activity"
- obtain a copy of your free credit report
- contact the FTC and/or the state Attorney General's office to report misuse of your personal information
- or to obtain additional information about avoiding identity theft

None of these recommendations, however, requires Defendants to expend any effort to protect Plaintiffs' and Class Members' PI, fails to provide monetary compensation, and provides no protection whatsoever after 12 months.

118. Defendants' disclosure of their driver's license numbers directly to members of the public with small amounts of Plaintiffs' PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Defendants' Notice indicates, they are putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

119. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come.

120. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PI for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

121. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

122. Industry experts are clear that a data security incident is indicative of data security failures. Indeed, though GEICO's knowing Data Disclosure is more egregious than a data breach, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance . . . ."[34]

123. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, because of GEICO's Data Disclosure and the fact that their driver's license numbers are now in the hands of criminals, including but not limited to: invasion of privacy; loss of privacy; loss of control over PI and

---

[33] *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, at 29, *see supra* at n.33 (emphasis added).

[34] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, Reuters (May 26, 2017) http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited May 20, 2022).

identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PI; harm resulting from damaged credit scores and credit information; a substantially increased risk of future identity theft and fraud; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized disclosure of PI.

CLASS ALLEGATIONS

124. Plaintiffs bring this action on behalf of themselves and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States whose driver's license information was disclosed in the GEICO Data Disclosure occurring in or around the period between November 24, 2020 and March 1, 2021, including all persons who received notice of the GEICO Data Disclosure.
>
> **New York Class**
> All residents of New York whose driver's license information was disclosed in the GEICO Data Disclosure occurring in or around the period between November 24, 2020 and March 1, 2021, including all persons who received notice of the GEICO Data Disclosure.

125. The above defined classes are collectively referred to as the "Class" or "Classes." Plaintiffs reserve the right to re-define the Class(es) prior to class certification. Plaintiffs reserve the right to modify these class definitions as discovery in this action progresses.

126. Excluded from the Class are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

127. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable,

as the proposed Classes appear to include many thousands of members who are geographically dispersed.

128. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members he seeks to represent. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

129. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests are aligned with the Classes they seek to represent and they have no conflicts of interest with the Classes. Plaintiffs' Interim Co-Lead Class Counsel are competent with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and Plaintiffs' Interim Co-Lead Class Counsel intend to prosecute this action vigorously. The Classes' interests are well-represented by Plaintiffs and Plaintiffs' Interim Co-Lead Class Counsel.

130. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer

management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

131. **Commonality and Predominance**: The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants knowingly used Plaintiffs' and the Class Members' driver's license numbers to sell auto insurance;
- whether Defendants knowingly disclosed Plaintiffs' and the Class Members' driver's license numbers;
- whether Defendants violated the DPPA;
- whether Defendants' data security practices and the vulnerabilities of GEICO's systems resulted in the disclosure of Plaintiffs' and other Class Members' sensitive information;
- whether Defendants violated privacy rights and invaded Plaintiffs' and Class Members' privacy (intrusion upon seclusion);
- whether Defendants were negligent or negligent *per se* when they disclosed the sensitive information of Plaintiffs and other Class Members;
- whether Defendants violated the New York GBL when they disclosed Plaintiffs' and other Class Members' sensitive information, including their driver's license numbers; and
- whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

132. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the Classes, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
Violation of the Drivers' Privacy Protection Act, 18 U.S.C. § 2724, *et seq.*
(On behalf of Plaintiffs and the Nationwide Class, or in the alternative, the New York Class)

133. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

134. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Class.

135. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains. . . ." 18 U.S.C. § 2724.

136. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

137. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Drivers' license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

138. Defendants obtain, use and disclose motor vehicle records from its customers.

139. Defendants also obtain motor vehicle records directly from state agencies or through resellers (third party prefill services) who sell such records.

140. Defendants knowingly used the above described information to sell auto insurance on its free online sales system, accessible from www.GEICO.com.

141. Defendants knowingly published the above described information to the public on their free online sales system, accessible from www.GEICO.com.

142. Defendants knowingly linked their respective public websites to systems and/or networks storing maintaining, and/or obtaining Plaintiffs' and Class Members' PI.

143. GEICO had a practice of offering online insurance quotes to applicants long before it incorporated this auto-population feature, but added the auto-population feature to its online sales system in order to gain competitive advantage in its sales process. By adding the auto-population feature to its online quoting process, which GEICO knowingly chose to do, GEICO knew that it was using the driver's license information to sell insurance and making the displayed information easily accessible to anyone who entered basic information into its system. GEICO did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. GEICO did not impose effective security protocols to prevent automated bots from accessing consumers' PI.

144. During the time period up until at least March 1, 2021, PI, including drivers' license numbers, of Plaintiffs and Class Members, were publicly available and viewable on Defendants' online sales system, and Defendants knowingly obtained, used, and disclosed and/or redisclosed Plaintiffs' and Class Members' motor vehicle records and PI to the general public, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

145. Pursuant to the allegations herein, GEICO knew, inferably knew, or should have known that it obtained, disclosed, and used personal information, from a motor vehicle record, for a purpose not permitted under the DPPA.

146. By engaging in the conduct described above, Defendants knowingly obtained personal information for a purpose not permitted under the DPPA.

147. By engaging in the conduct described above, Defendants knowingly used personal information for a purpose not permitted under the DPPA.

148. By engaging in the conduct described above, Defendants knowingly disclosed or re-disclosed personal information for a purpose not permitted under the DPPA.

149. As a result of GEICO's acquisition, use, subsequent Data Disclosure, and violations of the DPPA, Plaintiffs and putative Class Members are entitled to statutory damages to maximum allowable, actual damages, liquidated damages, and attorneys' fees and costs.

COUNT II
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, the New York Class)

150. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

151. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Class.

152. Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing their data security systems to ensure Plaintiffs' and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

153. Defendants owed a duty to Plaintiffs and the Class Members to adopt, implement, and maintain a process by which it could detect vulnerabilities in its websites and systems in a

reasonably expeditious period of time and to give prompt notice in the case of a data security incident, including an unauthorized use of data knowingly disclosed on Defendants' website.

154. Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that their systems and networks—and the personnel responsible for them—adequately protected PI it stored, maintained, used, accessed, and/or obtained.

155. Defendants further assumed the duty to implement reasonable security measures as a result of its general conduct, internal policies and procedures, in which GEICO states, among other things, that GEICO.com's "[p]hysical safeguards, procedural controls and data access controls protect your data from unauthorized access" and GEICO "continually monitor[s] our systems to prevent unauthorized attempts at intrusion." Through these statements, GEICO specifically assumed the duty to comply with industry standards in protecting its customers' and other consumers' PI; and to adopt, implement, and maintain internal standards of data security that met those industry standards.

156. Unbeknownst to Plaintiffs and Class Members, they were entrusting Defendants with their PI when Defendants obtained their PI from motor vehicle records directly from state agencies or through resellers or third party prefill services who sell such records. Defendants had an obligation to safeguard Plaintiffs' and Class Members' PI and were in a position to protect against the harm suffered by Plaintiffs and Class Members, instead GEICO chose to disclose Plaintiffs' and Class Members' driver's license numbers so it could sell more auto insurance.

157. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote

requests with private PI without the consent or authorization of the person whose PI was being provided. Only GEICO was in a position to ensure that its systems were sufficient to protect against harm to Plaintiffs and the Class resulting from a data security incident, instead it chose to disclose Plaintiffs' and Class Members' driver's license numbers so it could sell more auto insurance.

158. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent disclosure of PI, instead GEICO chose to disclose Plaintiffs' and Class Members' driver's license numbers.

159. Defendants acknowledge their conduct created actual harm to Plaintiffs and Class Members because Defendants warned of potential fraudulent unemployment benefits claims in their names as a result of their Data Disclosure and offered one year of credit monitoring.

160. Defendants knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

161. Because Defendants knew that their disclosure of sensitive PI would damage thousands of individuals, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

162. Defendants breached their duties to Plaintiffs and Class Members, and thus were negligent, by failing to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiffs' and Class Members' PI, failing to adequately monitor the security of GEICO's online sales system and website, knowingly providing Plaintiffs' and Class Members'

driver's license information directly to members of the public with small amounts of their PI, failing to recognize in a timely manner that Plaintiffs' and Class Members' PI had been disclosed, and failing to warn Plaintiffs and Class Members in a timely manner that their PI had been disclosed.

163. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

164. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' PI.

165. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and the Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the disclosure of their PI.

166. Neither Plaintiffs nor the other Class Members contributed to GEICO's Data Disclosure.

167. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or fraudulent use of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of GEICO's Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of

privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or to which Defendants continue to have access) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PI.

168. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' PI.

169. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class,
or in the alternative, the New York Class)

170. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

171. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Class.

172. Defendants also had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiffs' and Class Members' PI. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45) and the GLB Act (15 U.S.C. § 6801 *et seq.*), GEICO had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs' and Class Members' PI. Further, pursuant to the Federal Trade Commission Act (15 U.S.C. § 45) and N.Y. Gen. Bus. Law § 349, Defendants had a duty to provide fair, reasonable, or adequate data

security in connection with the sale of insurance policies and use of the GEICO website in order to safeguard Plaintiffs' and Class Members' PI.

173. In engaging in the knowing and/or negligent acts and omissions as alleged herein, in which GEICO disclosed Plaintiffs' and Class Members' PI to malicious hackers through GEICO's online sales system, Defendants violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce," and the GLB Act. This includes failing to have adequate data security measures and failing to protect Plaintiffs' and the Class Members' PI. Defendants also breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and N.Y. Gen. Bus. Law § 349, among other statutes, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiffs' and Class Members' PI in connection with the use of the GEICO website and online sales system.

174. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

175. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

176. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PI.

177. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV
Violations of New York General Business Law
N.Y. Gen. Bus. Law § 349 ("GBL")
(On Behalf of Plaintiffs and the New York Class)

178. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

179. Plaintiffs bring this cause of action individually and on behalf of the New York Class.

180. Section 349 of the New York GBL provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." N.Y. Gen. Bus. Law § 349(a).

181. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. disclosing Plaintiffs' and Class Members' PI;

b. failing to enact adequate privacy and security measures to protect Plaintiffs' and Class Members' PI from unauthorized disclosure, release, and theft;

c. failing to take proper action following known security risks and prior cybersecurity incidents;

d. knowingly and fraudulently providing Plaintiffs' and Class Members' driver's license information directly to members of the public with small amounts of their PI;

e. omitting, suppressing, and concealing the inadequacy of Defendants' security protections;

f. knowingly and fraudulently misrepresenting that Defendants would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of PI, and

g. failing to disclose their Data Disclosure to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

182. As a direct and proximate result of Defendants' practices, including their Data Disclosure, Plaintiffs and other Class Members suffered injury and/or damages, including but not limited to actual misuse of their PI, fraud, and identity theft; lost time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PI.

183. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and other Class Members that they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

184. In view of their decision to disclose the PI in their Data Disclosure, Defendants knew or should have known that their systems and data security practices were inadequate to safeguard PI entrusted to it, and that risk of fraudsters obtaining the PI was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts, including GEICO's Data Disclosure, were negligent, knowing and willful.

185. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

186. Plaintiffs and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions, in that Defendants will continue to fail to protect PI entrusted to them, as detailed herein.

187. Plaintiffs and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendants from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

COUNT V
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiffs and the Nationwide Class
or, in the alternative, the New York Class)

188. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

189. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Class.

190. Plaintiffs and Class Members had a reasonable expectation of privacy in the PI that Defendants disclosed without authorization.

191. By knowingly using and disclosing Plaintiffs' and Class Members' PI, disclosing the PI to unauthorized parties for unauthorized use, failing to keep Plaintiffs' and Class Members' PI safe, utilizing unsecure systems, and Defendants unlawfully invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

a. intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiffs' and Class Members' privacy by improperly using their PI properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure their PI from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiffs' and Class Members' PI without consent.

192. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

193. Defendants knew that their decision to disclose the PI on their website, in the manner in which it was disclosed, was vulnerable to fraudsters' who could easily access the PI, and that GEICO's systems were vulnerable prior to their Data Disclosure.

194. Defendants invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their driver's license information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

195. As a proximate result of GEICO's Data Disclosure, Plaintiffs' and Class Members' reasonable expectations of privacy in their PI was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

196. In failing to protect Plaintiffs' and Class Members' PI, and in disclosing Plaintiffs' and Class Members' PI, Defendants acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

197. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

COUNT VI
Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class
or, in the alternative, the New York Class)

198. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

199. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or in the alternative, the New York Class.

200. As previously alleged, Plaintiffs and Class Members have a reasonable expectation that companies such as Defendants, who could access their PI through automated systems, would provide adequate security for that PI.

201. GEICO owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PI.

202. Defendants still possess and can still access PI regarding Plaintiffs and Class Members.

203. Since their Data Disclosure, Defendants have announced few, if any changes to their decision to disclose the PI, their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems or online sales system.

204. GEICO's Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that led to such exposure.

205. There is no reason to believe that Defendants' security measures are more adequate now to meet Defendants' legal duties than they were before their Data Disclosure.

206. Plaintiffs therefore seek a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendants not to disclose PI, including driver's license information, to the general public through their website or sales platforms;

b. Ordering Defendants to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated inquiries by bots, simulated cyber-attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

c. Ordering Defendants to engage third–party security auditors and internal personnel to run automated security monitoring, including risk analysis on GEICO's decision making,

d. Ordering Defendants to audit, test, and train its security personnel regarding any new or modified procedures,

e. Ordering Defendants not to make PI available on their instant quote webpage,

f. Ordering Defendants not to store PI or make PI accessible in any publicly facing website,

g. Ordering Defendants to purge, delete, and destroy in a reasonably secure manner customer and consumer data not necessary for their provisions of services,

h. Ordering Defendants to conduct regular computer system scanning and security checks; and

i. Ordering Defendants routinely and continually to conduct internal training and education to inform employees and officers on PI security risks, internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a data security incident.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Classes, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as the class representative and Plaintiffs' Interim Co-Lead Class Counsel as class counsel;

B. Award Plaintiffs and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: May 20, 2022

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON (NY Bar No. 5436043)
DEBORAH DE VILLA (NY Bar No. 5724315)
AHDOOT & WOLFSON, PC
100 Avenue of the Americas, 9th Floor
New York, NY 10013
Telephone: (917) 336-0171
Facsimile: (917) 336-0177
twolfson@ahdootwolfson.com
ddevilla@ahdootwolfson.com

ROBERT AHDOOT
(admitted *pro hac vice*)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
rahdoot@ahdootwolfson.com

Dated: May 20, 2022

/s/ E. Michelle Drake

E. MICHELLE DRAKE
(admitted *pro hac vice*)
JOSEPH C. HASHMALL
(*pro hac vice* forthcoming)
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5999
Facsimile: (612) 584-4470
emdrake@bm.net
jhashmall@bm.net

Interim Co-Lead Class Counsel

Dated: May 20, 2022

/s/ Karen Hanson Riebel

KAREN HANSON RIEBEL
(admitted *pro hac vice*)
KATE M. BAXTER-KAUF
(admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Additional Counsel for Plaintiffs

ATTESTATION OF FILER

I hereby attest that all signatories above have reviewed and concur with the filings of this document.

Dated: May 20, 2022

/s/ Tina Wolfson
Tina Wolfson